

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-110193

(43)Date of publication of application : 23.04.1999

(51)Int.Cl.

G06F 9/06

(21)Application number : 09-265882

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 30.09.1997

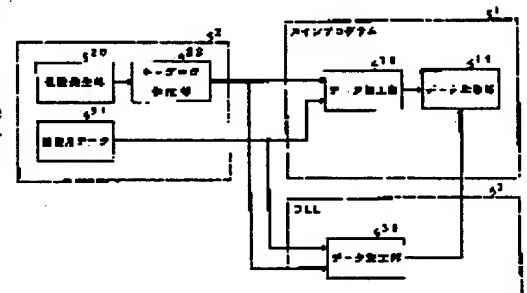
(72)Inventor : TAKAHASHI MASAKI

(54) COMPUTER SYSTEM AND LIBRARY LINK METHOD APPLIED TO THE COMPUTER SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To realize a link function with a normal library by means of a library authentication function, and accordingly, to prevent forgery of library.

SOLUTION: In the computer system having a DLL(dynamic link library) function, a main program 1 inputs the authentication data and the key data to a data processing part 10 from a data generation part 2 included in an authentication function and also gives these two data to a data processing part 30 included in the authentication function of a DLL 3. A data comparison part 11 of the program 1 compares the 1st and 2nd processing data obtained from both parts 10 and 30 with each other. When both processing data are coincident with each other, the DLL 3 is authenticated as a normal library.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

...

;

~

→

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-110193

(43) 公開日 平成11年(1999) 4月23日

(51) Int.Cl.⁶

G 0 6 F 9/06

識別記号

4 1 0

F I

G 0 6 F 9/06

4 1 0 E

審査請求 未請求 請求項の数 9 O L (全 6 頁)

(21) 出願番号 特願平9-265882

(22) 出願日 平成9年(1997) 9月30日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 高橋 正樹

東京都青梅市末広町2丁目9番地 株式会
社東芝青梅工場内

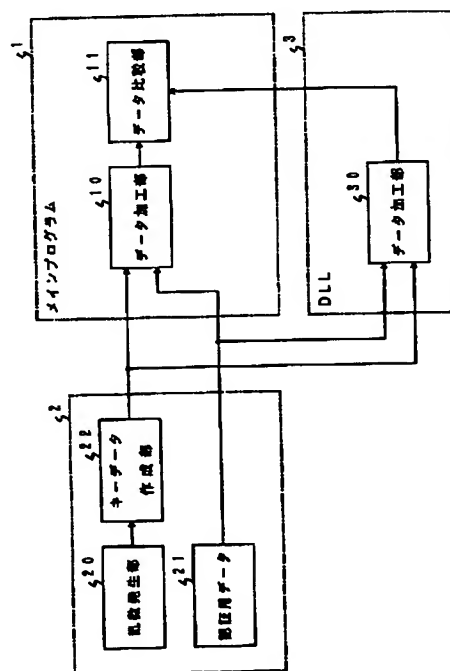
(74) 代理人 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 コンピュータシステム及び同システムに適用するライブラリのリンク方法

(57) 【要約】

【課題】 ライブラリに対する認証機能により正規のライブラリとのリンク機能を実現して、結果的にライブラリの偽造防止を図ることにある。

【解決手段】 ダイナミック・リンク・ライブラリ機能を有するコンピュータシステムにおいて、メインプログラム1は認証用関数に含まれるデータ生成部2から認証用データとキーデータをデータ加工部10に入力すると共に、DLL3の認証用関数に含まれるデータ加工部30に同一の認証用データとキーデータを与える。メインプログラム1側のデータ比較部11は、各データ加工部10, 30から得られた第1と第2の加工処理データとを比較し、一致した場合にDLL3を正規のライブラリとして認証する。



1

【特許請求の範囲】

【請求項 1】 実行対象のプログラムと予め用意されたライブラリとをリンク処理するためのリンク機能を有するコンピュータシステムであって、

リンク対象のライブラリを認証するための認証用データを生成するための生成手段と、

前記認証用データを当該プログラム及び当該ライブラリのそれぞれに設定するための設定手段と、

当該プログラムと当該ライブラリとのリンク処理時に、当該プログラムに設定した認証用データと当該ライブラリに設定した認証用データとを比較して、比較結果が一致した場合には当該ライブラリが当該プログラムのリンク対象のライブラリであることを認証する認証手段とを具備したことを特徴とするコンピュータシステム。

【請求項 2】 実行対象のプログラムと予め用意されたライブラリとのリンク処理するためのリンク機能を有するコンピュータシステムであって、

リンク対象のライブラリを認証するための認証用データ及び前記認証用データをデータ加工処理するためのキーデータを生成するための生成手段と、

前記認証用データ及び前記キーデータを当該プログラム及び当該ライブラリのそれぞれに設定するための設定手段と、

当該プログラムに設定された前記キーデータに従って前記認証用データをデータ加工処理するための第 1 のデータ加工手段と、

当該ライブラリに設定された前記キーデータに従って前記認証用データをデータ加工処理するための第 2 のデータ加工手段と、

当該プログラムと当該ライブラリとのリンク処理時に、前記第 1 のデータ加工手段により得られた加工処理データと前記第 2 のデータ加工手段により得られた加工処理データとを比較して、比較結果が一致した場合にはリンク対象のライブラリであることを認証する認証手段とを具備したことを特徴とするコンピュータシステム。

【請求項 3】 前記ライブラリはダイナミック・リンク・ライブラリであり、

前記リンク機能はプログラムの実行時に当該プログラムと前記ライブラリとを動的にリンク処理することを特徴とする請求項 1 または請求項 2 記載のコンピュータシステム。

【請求項 4】 前記ライブラリはダイナミック・リンク・ライブラリであり、

前記リンク機能は、前記認証手段により認証された当該ライブラリと当該プログラムとを動的にリンク処理し、前記認証手段により認証されない場合には所定のエラー処理を実行する手段を有することを特徴とする請求項 1 または請求項 2 記載のコンピュータシステム。

【請求項 5】 前記生成手段は、前記リンク機能を含むプログラム制御を実行するためのシステム制御手段に含

2

まれていることを特徴とする請求項 1 または請求項 2 記載のコンピュータシステム。

【請求項 6】 前記生成手段、前記設定手段、前記第 1 のデータ加工手段及び前記認証手段は当該プログラムにより呼出し可能な特定関数からなり、

前記第 2 のデータ加工手段は当該ライブラリに含まれる特定関数からなることを特徴とする請求項 2 記載のコンピュータシステム。

【請求項 7】 実行対象のプログラムと予め用意されたライブラリとのリンク処理するためのリンク機能を有するコンピュータシステムに適用するライブラリのリンク方法であって、

リンク対象のライブラリを認証するための認証用データ及び前記認証用データをデータ加工処理するためのキーデータを生成するステップと、

前記認証用データ及び前記キーデータを当該プログラム及び当該ライブラリのそれぞれに設定するステップと、当該プログラムに設定された前記キーデータに従って前記認証用データをデータ加工処理して第 1 の加工処理データを生成するステップと、

当該ライブラリに設定された前記キーデータに従って前記認証用データをデータ加工処理して第 2 の加工処理データを生成するステップと、

当該プログラムと当該ライブラリとのリンク処理時に、前記第 1 の加工処理データと前記第 2 の加工処理データとを比較して、比較結果が一致した場合にはリンク対象のライブラリであることを認証するステップと、

認証された当該ライブラリと当該プログラムとを動的にリンク処理するステップとからなることを特徴とするライブラリのリンク方法。

【請求項 8】 実行対象のプログラムと予め用意されたライブラリとのリンク処理するためのリンク機能を有するコンピュータシステムにより読取り可能な記憶媒体であって、

リンク対象のライブラリを認証するための認証用データ及び前記認証用データをデータ加工処理するためのキーデータを生成するステップと、

前記認証用データ及び前記キーデータを当該プログラム及び当該ライブラリのそれぞれに設定するステップと、

当該プログラムに設定された前記キーデータに従って前記認証用データをデータ加工処理して第 1 の加工処理データを生成するステップと、

当該ライブラリに設定された前記キーデータに従って前記認証用データをデータ加工処理して第 2 の加工処理データを生成するステップと、

当該プログラムと当該ライブラリとのリンク処理時に、前記第 1 の加工処理データと前記第 2 の加工処理データとを比較して、比較結果が一致した場合にはリンク対象のライブラリであることを認証するステップと、

認証された当該ライブラリと当該プログラムとを動的に

3

リンク処理するステップとを前記コンピュータシステムが実行するように設定されたプログラムを記憶した記憶媒体。

【請求項 9】 認証用データ及び前記キーデータを生成するためのステップ、前記認証用データ及び前記キーデータを当該プログラム及び当該ライブラリのそれぞれに設定するステップ、前記第 1 の加工処理データを生成するステップおよび前記認証するステップはそれぞれ当該プログラムにより呼出し可能な特定関数により実行される処理であり、

前記第 2 の加工処理データを生成するステップは当該ライブラリに含まれる特定関数により実行される処理であることを特徴とする請求項 8 記載の記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、特にダイナミック・リンク・ライブラリ機能を有するコンピュータシステムに関する。

【0002】

【従来の技術】従来、パーソナルコンピュータなどのコンピュータシステムにおいて、汎用的に利用されるルーチン（routine）の再利用、システム機能の拡張、またはソフトウェア開発の作業分担などの理由から、特定機能毎のプログラムをモジュール単位に開発し、一つのファイルとして設定されるライブラリと称する機能が設けられている。

【0003】ライブラリは、例えば標準的なサブルーチン群を構成する複数のオブジェクト・モジュール（メンバ）がコンパイルされて、一つのファイルとしてパッケージされたものである。システムは、通常ではリンクにより実行対象のプログラム（以下ライブラリのプログラム群と区別するためにメインプログラムと呼ぶ）とライブラリとをリンクして実行する。

【0004】ここで、ライブラリは、スタティック・リンク・ライブラリとダイナミック・リンク・ライブラリ（以下DLLと呼ぶ場合がある）とに大別される。前者はプログラムの実行前にリンクされるライブラリであり、後者はプログラムの実行時に動的にリンクされるライブラリである。特に、DLLは、複数のメインプログラムの共有ライブラリとして機能させることができるなどの利点を備えている。

【0005】

【発明が解決しようとする課題】ダイナミック・リンク・ライブラリ（DLL）は、複数のメインプログラムが実行中に同じライブラリを共有できるなどの利点がある。しかしながら、そのようなDLLを利用するシステムでは、例えば第三者が呼出し規則の等しいDLLを偽造した場合に、メインプログラムであるアプリケーション・プログラムは想定している機能とは異なる機能のライブラリとリンクして、本来の仕様とは異なったプロ

4

ラムとして動作する可能性がある。

【0006】このため、特にセキュリティ確保に係るDLLが偽造された場合に、パスワードなどの機密情報の漏洩、プログラムやデータのコピー防止機能の解除（著作権の侵害を招く）、またはプログラムの暴走などによるシステム破壊などが発生する可能性がある。

【0007】そこで、本発明の目的は、ライブラリに対する認証機能により正規のライブラリとのリンク機能を実現して、結果的にライブラリの偽造防止を図ることに10 ある。

【0008】

【課題を解決するための手段】本発明は、特にダイナミック・リンク・ライブラリ機能を有するコンピュータシステムにおいて、リンク対象のライブラリを認証するための認証用データを生成するための生成手段と、認証用データをメインプログラム（アプリケーション・プログラム）及び当該ライブラリのそれぞれに設定するための設定手段と、当該認証用データに基づいて当該ライブラリが正規のリンク対象のライブラリであることを認証する20 認証手段とを有するシステムである。

【0009】具体的には、当該メインプログラム及び当該ライブラリはそれぞれ、予め用意された認証用関数（特定機能ルーチン）を呼出し、認証用データの生成処理、認証用データの設定処理、及び認証処理を実行する。当該メインプログラムでは、認証用関数が生成した認証データとリンク対象の当該ライブラリからの認証データとを比較し、比較結果が一致であれば正規のライブラリとして認証する。この認証結果に基づいて、当該メインプログラムと当該ライブラリとのリンク処理が実行30 される。このような方式により、仮に偽造されたライブラリが設定されている場合に、前記の認証処理によりメインプログラムに対するリンク対象ライブラリから偽造ライブラリを除去することが可能となる。

【0010】本発明の別の観点として、リンク対象のライブラリを認証するための認証用データ及び認証用データをデータ加工処理するためのキーデータを生成するための生成手段と、認証用データ及びキーデータを当該プログラム及び当該ライブラリのそれぞれに設定するための設定手段と、当該プログラムに設定されたキーデータ40 に従って認証用データをデータ加工処理するための第1のデータ加工手段と、当該ライブラリに設定されたキーデータに従って認証用データをデータ加工処理するための第2のデータ加工手段と、第1のデータ加工手段により得られた加工処理データと第2のデータ加工手段により得られた加工処理データとを比較して、比較結果が一致した場合にはリンク対象のライブラリであることを認証する認証手段とを有するシステムである。

【0011】このようなシステムであれば、認証用データはキーデータに基づいて暗号化処理に相当するデータ50 加工処理される。従って、仮に認証用データが第三者に

5

漏洩されても、認証手段は認証用データそのものではなく、データ加工処理により得られた加工処理データに基づいて認証処理を実行するため、第三者に対するセキュリティを確保することができる。

【0012】

【発明の実施の形態】以下図面を参照して本発明の実施の形態を説明する。図1は本実施形態に係るシステムの概念を示すブロック図であり、図2は同実施形態に係るリンク処理を説明するための概念図であり、図3は同実施形態に係るコンピュータシステムのハードウェア構成を示すブロック図であり、図4は同実施形態のリンク処理を説明するためのフローチャートである。

（システム構成）本実施形態は、アプリケーション・プログラムであるメインプログラム1が実行時に、予め用意されたダイナミック・リンク・ライブラリ（DLL）3と動的にリンクする機能を有するコンピュータシステムを想定する。

【0013】メインプログラム1とDLL3はそれぞれ、予め用意された認証用関数（特定機能ルーチン）を呼出して実行させる機能を有する。メインプログラム1側の認証用関数は、図1に示すように、認証用データとキーデータを生成するためのデータ生成部2、データ加工部10及びデータ比較部11の各機能に大別する。データ生成部2は、認証データを生成する認証データ生成部21とキーデータ作成部22とを有する。キーデータ作成部22は、乱数発生部20により生成される乱数データに基づいて、予め設定された認証データを加工処理（暗号化処理）するためのキーデータを作成する。

【0014】データ加工部10は、キーデータ作成部22からのキーデータに基づいて、所定のアルゴリズムにより認証データ生成部21からの認証データを加工処理（暗号化処理）する。一方、DLL3側の認証用関数は、メインプログラム1側と同一機能のデータ加工部30を有する。データ生成部2は、メインプログラム1側のデータ加工部10と同一の認証データとキーデータを与える。DLL3側のデータ加工部30は、データ加工部10と同様に、キーデータに基づいて所定のアルゴリズムにより認証データを加工処理（暗号化処理）する。

【0015】データ比較部11は、データ加工部10により得られる加工処理データ（暗号化された認証データであり、以下第1の加工処理データと呼ぶ）とDLL3側のデータ加工部30により得られる加工処理データ（以下第2の加工処理データと呼ぶ）とを比較し、比較結果が一致の場合にメインプログラム1とDLL3とをリンクさせるリンク処理を実行させる。

【0016】ここで、コンピュータシステムのハードウェア構成としては、図3に示すように、CPU40と、メインメモリ41と、外部記憶装置42と、システムバス43とを有する例えばパーソナルコンピュータを想定

6

する。メインメモリ41には、メインプログラム1、DLL3、OS（オペレーティングシステム）、及びリンカなどのソフトウェアツールがロードされる。CPU40は、メインメモリ41に格納されたメインプログラム1を実行し、かつリンクされたDLL3を実行する。外部記憶装置42は、メインプログラム1、DLL3、OS（オペレーティングシステム）、及びリンカなどのソフトウェアツールをファイルとして保存するためのファイル装置である。

10（本実施形態のリンク処理）以下図1と図2、及び図4のフローチャートを参照して本実施形態のリンク処理について説明する。

【0017】まず、通常ではアプリケーション・プログラムであるメインプログラム1が実行時にDLL3にリンクする場合には、リンカ（ダイナミック・リンカ）に制御を移す。即ち、図2に示すように、リンカ100はリンク情報に基づいて、メインプログラム1とDLL3とをリンクさせる。このリンク処理が終了すると、メインプログラム1に制御が移行して、メインプログラム120はリンクしたDLL3のプログラムモジュール（特定機能のサブルーチンなど）と共に、所定のデータ処理を実行する。

【0018】このようなリンク機能の実行前に、本実施形態のメインプログラム1は認証用関数を呼出し、データ生成部2により認証用データとキーデータの生成処理を実行させる（ステップS1、S2）。さらに、メインプログラム1はDLL3の認証用関数を呼出し、当該関数に含まれるデータ加工部30に認証用データとキーデータとを与える（ステップS3）。

30【0019】メインプログラム1側のデータ加工部10は、キーデータに基づいて所定のアルゴリズムにより認証データを加工処理して、第1の加工処理データ（暗号化データ）を生成する（ステップS4）。一方、DLL3側のデータ加工部30も、キーデータに基づいて所定のアルゴリズムにより認証データを加工処理して、第2の加工処理データを生成する。

【0020】データ比較部11は、データ加工部10により得られる第1の加工処理データとDLL3側のデータ加工部30により得られる第2の加工処理データとを比較し、比較結果が一致の場合にはDLL3を正規のDLLとして認証する（ステップS5、S6）。データ比較部11は、DLL3を正規のDLLとして認証した場合には、前記のようにメインプログラム1とDLL3とをリンクさせるリンク処理を実行させる（ステップS7、図2を参照）。ここで、データ比較部11は、比較結果が不一致の場合には、所定のエラー処理を実行させる（ステップS6のNO、S8）。即ち、メインプログラム1はDLL3とのリンク処理が不可となる。

【0021】以上のように本実施形態によれば、あるアプリケーション・プログラムであるメインプログラム1

50

7

が、実行時にDLL3と動的にリンクする場合に、予め用意された認証用関数により、リンク対象のDLL3が正規のDLLであるか否かを認証する。この場合、正規のDLLには、認証用関数としてデータ加工部30が設けられて、このデータ加工部30にはメインプログラム1のデータ加工部10と同一の認証データとキーデータとが与えられる。

【0022】ここで、認証用関数であるデータ加工部30を機密にすることにより、仮に第三者が偽造したDLLがシステムに設定されている場合に、この偽造DLLには認証用関数であるデータ加工部30が設けられていない。従って、メインプログラム1がリンク対象として偽造DLLが設定されても、メインプログラム1側のデータ比較部11は偽造DLLからは前記の第2の加工処理データが得られないため認証不可となる。このため、偽造DLLはリンク対象からは除かれることになる。換言すれば、リンク対象ライブラリから偽造ライブラリを除去できるため、メインプログラム1は常に正規のDLLとリンクし、必要な特定機能ルーチンを実行することができる。

【0023】なお、本実施形態において、データ生成部2は、メインプログラム1により呼出される認証用関数として説明したが、これに限る事なく、システムのOSの機能として動作してもよい。

【0024】

【発明の効果】以上詳述したように本発明によれば、ダイナミック・リンク・ライブラリ機能を有するコンピュータシステムにおいて、ライブラリに対する認証機能を実現することにより、常に正規のライブラリとのリンク処理を行なうことができる。従って、例えば第三者が呼

8

出し規則の等しいDLLを偽造した場合でも、その偽造DLLをリンク対象から外すことができる。これにより、アプリケーション・プログラムは常に想定している機能のライブラリとリンクして、必要な仕様を満足するプログラムとして動作することができる。

【図面の簡単な説明】

【図1】本発明の実施形態に関するコンピュータシステムの概念を示すブロック図。

【図2】同実施形態に関するリンク処理を説明するた10めの概念図。

【図3】同実施形態に関するコンピュータシステムのハードウェア構成を示すブロック図。

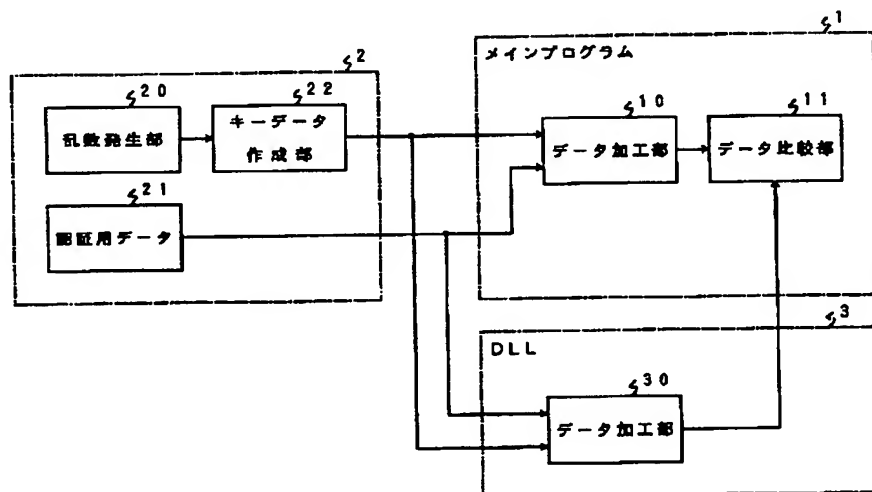
【図4】同実施形態のリンク処理を説明するためのフローチャート。

【符号の説明】

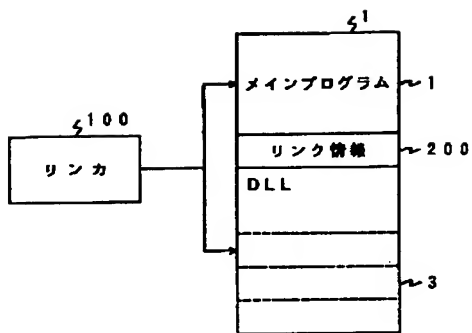
- 1…メインプログラム（アプリケーション・プログラム）
- 2…データ生成部
- 3…ダイナミック・リンク・ライブラリ（DLL）
- 2010…データ加工部（第1のデータ加工手段）
- 11…データ比較部
- 20…乱数発生部
- 21…認証用データ生成部
- 22…キーデータ作成部
- 30…データ加工部（第2のデータ加工手段）
- 40…CPU
- 41…メインメモリ
- 42…外部記憶装置
- 43…システムバス

30

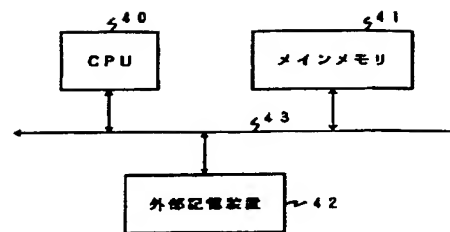
【図1】



【図2】



【図3】



【図4】

